STATE RECORDS COMMISSION

# SRC Standard 8

# MANAGING DIGITAL INFORMATION

**A Recordkeeping Standard for State Organizations**

**State Records Commission of WA**
**Perth, Western Australia**
**June 2016**

## TABLE OF CONTENTS

## PURPOSE

The purpose of this Standard, established under section 61 of the *State Records Act 2000*, is to describe requirements that must be satisfied in Recordkeeping Plans for State organizations to demonstrate good practice digital recordkeeping. It is not the intention of this document to prescribe that State organizations must move to digital recordkeeping, but to provide Principles for those that do keep information in a digital format.

This Standard supersedes *SRC Standard 8: Digital Recordkeeping*, 2008.

## BACKGROUND

State organizations create many state records and information in digital format. Managing digital information differs from managing physical information. At the lowest level, digital information is made up of binary encoded data that requires software to reveal its contents. Digital information is stored on a variety of digital media that is easily damaged and may be prone to obsolescence. Consequently, the storage of digital information both in terms of storage media and the file formats in which they are kept, must be managed with methods to ensure that the information is available and sufficient to meet accountability, business and archival requirements. In managing digital information, State organizations must also comply with the *State Records Act 2000*.

Digital information is any digitally produced or stored record of information within the meaning of section 3 of the *State Records Act 2000* and must be captured as evidence of business activity and stored into recordkeeping systems along with metadata that describes their content, structure and context. These requirements are set out in *SRC Standard 1: Government Recordkeeping* and *SRC Standard 2: Recordkeeping Plans*. Digital information must be managed to remain usable for as long as it is required. Access to digital information is regulated through legislation such as the *State Records Act 2000* and *Freedom of Information Act 1992*. Close attention to security mechanisms is essential to prevent unauthorized access or tampering with digital information. State organizations must plan for the recovery of lost data in the event of a disaster – loss of digital information can be crippling to the reconstruction of business activity.

Given the rapid obsolescence of technology, organizations should plan the preservation of digital information according to its required period of retention. Digital information that is to be retained on a long term basis by a State organization, or is to be transferred to the State archives collection, requires active and ongoing preservation to ensure its usability.

Digital information identified as State archives must be kept in a software file format and on media that is both viable and usable until it is transferred into the State archives collection.

Digital information of temporary value must be destroyed securely in accordance with an approved disposal authority and in such a way that it cannot be reconstructed.

## SCOPE

The principles and minimum compliance requirements in this Standard apply to all State organizations as defined in the *State Records Act 2000*.

The Standard describes specific requirements for the good practice management of digital information that is either born digital or has been created as a consequence of the digitization of physical source records.

## DEFINITIONS

Refer to the *Glossary of Terms* produced by the State Records Office of Western Australia available on the State Records Office website.

## Principle 1 – Managing Digital Information

**State organizations ensure that all digital information is managed appropriately.**

### Rationale

Digital information includes all types of business information created and maintained electronically. This may include (but is not limited to): email, web sites, databases, application systems, word processed documents, spreadsheets, social media and digital reproductions of physical records. State organizations should develop policies, procedures and business solutions for capturing this information and managing it for as long as it is required in corporate recordkeeping compliant systems.

### Minimum Compliance Requirements

State organizations must ensure that:

1. All matters relating to the management of digital information are contained within their Recordkeeping Plans.
2. In developing policies, procedures and solutions for the management of digital information, reference is made to relevant State Records Commission Standards and Guidelines produced by the State Records Office.

## Principle 2 – Appraisal, Retention and Disposal of Digital Information

**State organizations ensure that digital information is appraised and its retention and disposal is managed in accordance with approved disposal authorities.**

### Rationale

Digital information created by State organizations during the course of business is a State record for the purposes of the *State Records Act 2000.* Digital information must therefore be appraised in accordance with *SRC Standard 3: Appraisal of Records*, Principle 1 - Appraisal; and its retention and disposal managed in accordance with *SRC Standard 2: Recordkeeping Plans*, Principle 5 - Retention and Disposal.

Digital information needs to be kept until it is no longer required for any purpose. There are three general reasons information needs to be kept, namely:

- to support the efficient conduct of business;
- to meet the requirements of legislation and accountability; and
- to meet the expectations of the community.

State organizations should prepare strategies for efficient digital preservation solutions in accordance with Principle 4 – Storing Digital Information. Digital information that has been identified as State archives must be held in software file formats with the appropriate metadata and on media that is both viable and usable until such time as it is transferred to the State archives collection.

### Minimum Compliance Requirements

State organizations must ensure that:

1. Digital information is appraised in accordance with *SRC Standard 3: Appraisal of Records*, Principle 1 - Appraisal.
2. The retention and disposal of digital information is managed in accordance with *SRC Standard 2: Recordkeeping Plans*, Principle 5 - Retention and Disposal.
3. Destruction of digital information is authorized and conducted using appropriately secure methods of destruction, ensuring the information cannot be reconstructed.

## Principle 3 – Security of Digital Information

**State organizations ensure that effective security and authentication controls exist to ensure digital information is safe from intentional or unintentional damage and unauthorized tampering or alteration.**

### Rationale

Adequate security is essential for all State records. When implementing information systems, State organizations must take special care to ensure they are secure, reliable and capable of producing records that are acceptable for business, legal, audit and other purposes.

The nature of digital information can make it susceptible to alteration or deletion, whether intentionally or unintentionally. Alterations to digital information can be virtually undetectable, undermining its evidential value as a record. Digital information is easily copied and the taking of copies can be undetectable, potentially leading to unauthorized access to confidential and personally or commercially sensitive data. Information Security and Computer Security are both equally important in planning for secure digital information stores and application systems. Security controls should be in place at all levels, including physical, network, operating system and application level, for production and development systems as well as backup data.

State organizations must recognize that data stored offshore is potentially beyond the control of the State government, and must undertake appropriate risk assessments of the data before selecting storage or data centres, whether onshore or offshore. State organizations must also ensure that data stored with an outsourced provider meets the requirements of *SRC Standard 6: Outsourcing*.

### Minimum Compliance Requirements

State organizations must ensure that:

1. Information systems are protected to best practice security standards.
2. Procedures are in place to identify and respond to incidents or attempted security breaches of systems that create or store digital information.
3. Systems and protocols are in place to prevent unauthorized access to, or alteration of, digital information and ensure its authenticity.
4. Procedures ensure that security and authentication mechanisms such as encryption and digital rights management (DRM) do not inadvertently make digital information inaccessible in the long term.
5. Access to digital information is secured and auditable.

6. A risk assessment is undertaken before storing information or application systems offsite or offshore.

## Principle 4 – Storing Digital Information

**State organizations ensure that digital information is stored on appropriate media to ensure its ongoing usability.**

### Rationale

Digital information is vulnerable to loss, destruction, unauthorized copying and modification. To ensure the ongoing protection of digital information, State organizations require efficient and effective means of maintaining, handling, securing, and storing digital information over time. Policies, procedures and effective mechanisms for the storage of digital information should be an integral component of an organization's recordkeeping framework. Recordkeeping Plans should contain recovery and restoration procedures for digital information in compliance with *SRC Standard 2: Recordkeeping Plans*, Principle 4 – Preservation.

The storage arrangements for digital information, and the media type on which it is stored, should depend on risk assessments of the information and business requirements. To ensure the integrity, reliability and usability of information, policy and procedures are required for the:

- Selection of storage media and devices;
- Storage locations and conditions;
- Security;
- Refreshment of media;
- Migration of data; and
- Integrity checks.

Where information is held in an archive file format, organizations must ensure that these formats as well as the media they are stored on are able to be read for as long as the record or data is required to be held.

NB: Backups are suitable for disaster recovery but are not a viable long term storage solution.

## Minimum Compliance Requirements

State organizations must ensure that:

1. Digital information is stored on appropriate and durable media to ensure the information remains usable for as long as required.
2. Digital storage devices are subjected to regular integrity checks and periodically refreshed to prevent data loss through media degradation or obsolescence.
3. Backup or 'IT archive' file formats remain usable for as long as required.
4. Risk assessments are conducted on information and data prior to the selection of storage locations.

## Principle 5 - Digitization

**State organizations ensure that digitized information is as authentic, reliable and usable as the source material from which it is created.**

### Rationale

Digitization is the creation of a digital reproduction or likeness of an analogue file (printed paper, photograph, audio tape, etc). Whether a digital reproduction can stand in place of source material as proof of a business transaction, or as evidence, depends upon its authenticity, integrity, reliability and usability.

If a reproduction is intended to serve the same purpose as the source material, then the reproduction will need to be as usable, authentic and as reliable as the original. Reproductions are subject to the same requirements as any other digital information and therefore a State organization must have sufficient confidence in its digitization procedures to certify the authenticity of the reproductions. Where the digital reproductions need to be kept for the long term, they must be preserved in the file formats identified in the *Digitization Specification* produced by the State Records Office. The conditions for the process of creating digital reproductions of documents which involves the destruction of the source record are outlined in the *General Disposal Authority for Source Records*.

Where destruction of the source material is contemplated, State organizations must ensure that a risk assessment has been performed identifying risks and risk minimization strategies and that this risk assessment has been included in their Recordkeeping Plans.

### Minimum Compliance Requirements

State organizations must ensure that:

1. Any digitization which involves the destruction of source records is undertaken within the framework of the *General Disposal Authority for Source Records*.
2. Policy and procedures comprehensively describe digitization, security and quality assurance practices.

## RELATED DOCUMENTS

Standards Australia Limited and Standards New Zealand, *Australian/New Zealand Standard AS/NZS ISO 16175 Information and documentation - Principles and functional requirements for records in electronic office environments.* Standards Australia Limited, Sydney; Standards New Zealand, Wellington, 2012.

**For further information regarding this Standard please contact**
**State Records Office of WA**
**ph: 9427 3600**
**email: sro@sro.wa.gov.au**